APPLICATION FOR UNITED STATES LETTERS PATENT

For

METHOD FOR GENERATING AND LOOKING-UP TRANSACTION KEYS IN COMMUNICATION NETWORKS

Inventor:

Brant Candelore

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

32400 Wilshire Boulevard

Los Angeles, CA 90025-1026

(408) 720-8598

Attorney's Docket No.: 80398.P439

"Express Mail" mailing label number: EL 672751045US

Date of Deposit: 5/22/01

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner for Patents, Washington, D. C. 20231

Maureen R. Pettibone

(Typed or printed name of person mailing paper or fee)

Maureen R. Pettibone

(Signature of person mailing paper or fee)

5/22/01

(Date signed)

METHOD FOR GENERATING AND LOOKING-UP TRANSACTION KEYS IN COMMUNICATION NETWORKS

FIELD OF THE INVENTION

[0001] This application claims the benefit of United States Provisional Application No. 60/237,317, filed October 10, 2000.

BACKGROUND

[0002] Cable Set Top Boxes (STBs) may have two-way interactivity with the headend in a cable network. However, security problems such as privacy and denial of service exist. Some of the data may be snooped by someone observing the shared wire that is connected among homes in a neighborhood, for example. For this reason, cable modems have built-in message encryption hardware (such as Data Encryption Standard (DES) hardware) and scrambling/descrambling capability. The Digital Audio/Visual Council (DAVIC) Out-of-Band (OOB) uses a different signaling method than cable modems, and does not have its built-in DES scrambling/descrambling capability. STBs are being designed with both cable modem and DAVIC OOB capability, and some with just DAVIC OOB capability. This presents possible security problems. For example, in a denial of service attack, someone might attempt to replay messages sent from a neighbor's STB to the headend. An attacker might replay a VOD (video on demand) "restart" command to harass a customer watching VOD. Such an attack would cause the movie to start over and over. It is therefore desirable to perform a function to provide a privacy function for the DAVIC OOB.

DESCRIPTION OF THE INVENTION

[0003] A method and apparatus for generating keys to encrypt communication in a network using distinctive device identification. In an IP network, the invention makes use of the unique Media Access Control (MAC) address header information as the distinctive device identification.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The object features and advantages of the present invention will be apparent to one skilled in the art from the following Detailed Description in which:

[0005] **Figure 1** is a simplified block diagram of one embodiment of the present invention.

[0006] **Figure 2** is a simplified block diagram of the encoding and decoding function of the present invention.

[0007] **Figure 3** is a simplified block diagram illustrating one embodiment for the generation of keys used to encode data.

[0008] **Figure 4** is a flow chart illustrating one embodiment of the process of the present invention.

[0009] **Figure 5** is an illustration of a signaling message utilized in accordance with an embodiment of the present invention.

[0010] **Figure 6** illustrates an encrypted signaling message using a key generated in accordance with an embodiment of the present invention.

[0011] **Figure 7** is a simplified block diagram of one embodiment for encrypting data.

DETAILED DESCRIPTION

[0012] In the following description for purposes of explanation numerous details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that these specific details are not required in order to practice the present invention. In other instances, well-known electrical structures and circuits are shown in block diagram form, in order not to obscure the present invention unnecessarily.

[0013] The present invention provides a method and apparatus for generating a secure key which may be used to encode and decode data communicated across a network, such as a cable network.

[0014] One embodiment is simply illustrated by **Figure 1**. The service provider 10 communicates across a communication network 15 to the user's device 20. In one embodiment, the service provider 10 is a cable network. In another embodiment, the service provider may be, for example, a terrestrial broadcaster, a direct broadcast satellite

company, phone or Digital Subscriber Line (DSL) service provider or other source. The user's equipment 20 operates to process the received data and to provide access to the user. The data may include program content, system information, entitlement management messages, entitlement control messages, VOD signaling, Web pages, Email, and other data. In one embodiment, the user device 20 is a set top box (STB), which couples to a monitor or broadcast display device for providing audio/visual programming. This device may be separate or included within a broadcast device.

[0015] **Figure 2** is a simplified block diagram of one embodiment of an apparatus that operates in accordance with the teachings of the present invention. This apparatus would be included or connected to the headend 10 and set top box 20 such that data could be encoded at one device (e.g., 10) sent in encoded form across the network 15 to the second device 20 and decoded at the second device.

[0016] The apparatus 210 includes non-volatile storage 220, logic 230 and input-output 240. In one embodiment, the non-volatile storage medium 220 stores distinctive information for at least one key, corresponding to a device. In one embodiment, the distinctive information is an identification of the device. In one embodiment in which a device, such as a set top box, communicates with the headend of a cable service provider, the non-volatile storage medium located in the set top box stores the key that is generated from the device identification of the set top box. In one embodiment, this device identification is the MAC address. This provides a unique identifier, which ensures a unique key using the same algorithm to generate the key.

[0017] In one embodiment in which communications are performed on the Digital Audio/Visual Council (DAVIC) out-of-band (OOB) connection, a MAC address is delivered as part of the header source device address information of an IP (internet protocol) message.

[0018] In one embodiment, the logic 230 encodes data using the key and decodes encoded data using the key, wherein the key is determined or accessed in accordance to a corresponding device identification. In one embodiment, the logic may access a data base of device identifications and corresponding keys. This is useful, for example, in a device such as a cable system headend, which communicates with multiple devices such as set top boxes. The keys can be loaded into each user device, e.g. set-top box at factory configuration time, using a secret key generation algorithm known only to the factory

loader and network controlling entity. At the network controlling entity, the logic 230 determines the keys using the device identification and generation keys stored in the non-volatile memory 220. The secret key generation algorithm uses the distinct device identification and the generation keys in Figure 3. Later, the network controlling entity 10 does not have to store the keys only the algorithm. The algorithm is used to rederive the device keys based on the distinct device indentification received in a message.

[0019] All sensitive messages sent and received by the device can be sent encrypted using these keys.

[0020] One embodiment is illustrated in **Figure 3.** Although **Figure 3** illustrates one process and structure for generation of keys, other processes and structures may be used. The keys generated 305 and 310 may be used for hashing and signing a message or encrypting a message. The keys may be re-generated each time a particular device, e.g. STB, needs to be accessed by the network controlling entity, e.g. the cable headend. In the case the keys are used to hash and sign a message, it should be noted that it may be possible to only send part of the hash and still be secure in order to reduce the message payload. As already mentioned, the headend does not need to store a database of keys. The algorithm and generation keys can be used to rederive the keys using the particular device identifications. Furthermore, the logic illustrated, i.e. cipher functions and Exclusive OR functions are illustrative and not intended to limit the possible functions that may be implemented. Furthermore, the multistage process illustrated in **Figure 3** is an example of one embodiment. Fewer or more stages may be implemented to generate the key or keys utilized to encode data for secure communications.

[0021] **Figure 4** illustrates one embodiment of the method of the present invention. At step 405, the device identification is accessed. As noted earlier, the device identification may be a distinctive device identification, such as the MAC address delivered as part of the header source address information of an IP message. At step 410, data is encoded using a key generated using the device ID. At step 415, the encoded data is transmitted in a message to a receiving device, the message including the device ID, for example, in it's header. Using the device ID from the header, the receiving device accesses the key, step 420. As noted earlier, the receiving device may generate the key using the device ID, or may access, for example, from non-volatile

memory, the key corresponding to the device ID. At step 425 the receiving device decodes the encoded data of the message using the key.

[0022] Using the key or keys generated, a signaling message and Secure Hash Algorithm – version 1 (SHA-1) can be generated as illustrated in **Figure 5.** In this case, the STB Key may be hashed with the message, but not sent. At the receiving end, the same process is repeated to confirm the hash.

[0023] The keys, as illustrated in **Figure 6** may also be used to encode data in a message. It is also possible to add any number of additional stages to make it more difficult for a hacker to trial for the values STB 1 or 2 (or both). In **Figure 7**, an additional stage is added. Preferably the Key Generator value can be a random number. It may be chosen by either the network controlling entity or the set-top box. This value can be sent ahead of time, in the clear along with the message, or a value that is preloaded into the set-top box at factory creation time.

[0024] The invention has been described in conjunction with different embodiments. It is evident that numerous alternatives, modifications, variations and uses will be apparent to those skilled in the art in light of the forgoing description.